PURPOSE

This policy governs the use of the recording and privacy functions in teleconferencing applications used by the Michigan Department of Health and Human Services (MDHHS). These applications include, but are not limited to, Microsoft Teams or comparable products such as Zoom.

Users of teleconferencing applications in group settings involving MDHHS business includes employees, staff, contractors, students and other trainees, and volunteers. Users also include other persons whose conduct, in the performance of work for the MDHHS, are under the direct control of the MDHHS, whether or not they are paid by the MDHHS.

DEFINITIONS

Confidential Information

Sensitive information wherein unauthorized disclosure could cause serious financial, legal, or reputational damage to an agency or the State of Michigan (SOM). Confidential data may include personally identifiable information (PII) or confidential non-public information that relates to an agency's business.

Criminal Justice Information (CJI)

Federal Bureau of Investigation (FBI) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Electronic Protected Health Information (ePHI)

Protected Health Information that is transmitted or maintained in electronic form.

Federal Tax Information (FTI)

Information that consists of federal tax returns and return information (and information derived from it) covered by the confidentiality protections of the Internal Revenue Code (IRC). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS),

or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the Internal Revenue Service (IRS).

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (such as, name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.

Protected Health Information (PHI)

Individually identifiable health related information that is collected by a HIPAA covered entity or component and is transmitted by, or maintained in, electronic or any other form or medium.

SSA-Provided Information

Confidential information provided by the Social Security Administration (SSA).

Teleconferencing

A live, interactive audio or audio-visual meeting that ensues between geographically dispersed participants, using telephones, laptops, desktop computers, and specially designed tech-enabled meeting rooms, via State of Michigan networks or the internet.

Screenshot

Using technology to capture an image of the screen of a device (taking a picture of the screen, Windows snipping tool, etc.)

POLICY

MDHHS protects the privacy of Michigan citizens. Use of teleconferencing software and technologies heightens the criticality of privacy and the need to use the least invasive means of engaging in these alternative methods of conducting our activities. Existing law, regulations and policies that address privacy remain in effect including HIPAA, HITECH, IRS, SSA, MDHHS Employee Handbook, and other applicable policies and procedures drafted and adopted by MDHHS relating to the protection of confidential and restricted information.

Recording of Meetings Conducted via Teleconference

Meetings conducted by staff involving MDHHS business may be recorded provided the following conditions are met:

- The meeting session is recorded by the host or their designee.
- The session is recorded only through the teleconferencing application. The use of cell phones or other portable devices with analog or digital audio recording functionality is prohibited.
- At the beginning of the meeting, before recording can begin, the meeting host may, depending on the agenda and related subject matter, provide verbal notice that the meeting will be recorded and allow participants who do not wish to be recorded the opportunity to opt out.
- All participants agree to refrain from sharing confidential information, including but not limited to PII, CJI, FTI, PHI, SSA-provided information, case-specific information, or restricted data, in screenshots or any other form, during the meeting.

The above requirements must be communicated and enforced by the host.

Review and Management of Recordings

Immediately after the meeting has concluded, the host must review the recording, chat threads, and other related meeting content for confidential information, which must be redacted or deleted.

Recordings of meetings, minutes, transcripts, and related information must be securely handled in compliance with MDHHS security and privacy policies. All media remains subject to retention and disposal in compliance with MDHHS records management policies.

Privacy Controls

All meetings are required to use available controls (passcode, waiting room, etc.) to prevent unauthorized participants.

Recording notifications may not be disabled for any reason.

ROLES AND RESPONSIBILITIES:

The MDHHS security officer and privacy officer must determine roles and responsibilities for Compliance and Data Governance Bureau personnel to support implementation of this policy.

MDHHS workforce members are responsible for reading, understanding and complying with the requirements detailed in this and other Information security program policies.

ENFORCEMENT

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

REFERENCES

State Standards/Regulations:

MDHHS Policy Manuals

DMB Administrative Guide

DTMB/Work Resources/Policies, Standards and Procedures/IT Technical Policies, Standards and Procedures

1340.00.130.02 Acceptable Use of Information Technology

CONTACT

For additional information concerning this policy, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.